WHAT IS CLAIMED IS:

1. A method for providing secure external memory that stores instructions for a processor, comprising the steps of:

receiving a plurality of encrypted instructions into a buffer of the processor from the external memory;

decrypting the plurality of encrypted instructions substantially simultaneously using a selected decryption algorithm to produce a plurality of decrypted instructions; and

forwarding at least one decrypted instruction of the plurality of decrypted instructions to a processing area of the processor.

2. The method according to claim 1, wherein the plurality of encrypted instructions comprise a plurality of consecutive encrypted instructions.

3. The method according to claim 2, wherein said step of receiving a plurality of encrypted instructions into a buffer of the processor from the external memory comprises the step of receiving the plurality of consecutive encrypted instructions from a bus having

a width equivalent to that of each consecutive encrypted instruction of the plurality of consecutive encrypted instructions.

4. The method according to claim 3, wherein the width is equal to eight (8) bits.

5. The method according to claim 1, wherein the selected decryption algorithm comprises at least one of a data encryption standard (DES), a triple DES, and an advanced encryption standard (AES).

6. The method according to claim 1, wherein said step of decrypting the plurality of encrypted instructions substantially simultaneously using a selected decryption algorithm to produce a plurality of decrypted instructions comprises the step of decrypting the plurality of encrypted instructions using at least one modified decryption key, the at least one modified decryption key being formed responsive, at least partly, to at least a portion of an address associated with at least one encrypted instruction of the plurality of encrypted instructions.

7. The method according to claim 6, wherein the at least one modified decryption key is formed further responsive, at least partly, to at least one decryption key, the at least one decryption key generated using at least a pseudo-random number generator.

8. The method according to claim 1, further comprising the steps of:

transferring the plurality of decrypted instructions to another buffer;

delaying said step of forwarding at least one decrypted instruction of the plurality of decrypted instructions to a processing area of the processor until an instruction address requested by the processing area corresponds to an instruction address associated with the at least one decrypted instruction of the plurality of decrypted instructions; and

wherein said step of forwarding at least one decrypted instruction of the plurality of decrypted instructions to a processing area of the processor comprises the step of forwarding the at least one decrypted instruction of the plurality of decrypted instructions to the processing area of the processor from the another buffer when the instruction address requested by the processing area corresponds to the instruction address associated with the at least one decrypted instruction of the plurality of decrypted instructions.

9. The method according to claim 1, wherein the processing area of the processor comprises at least one of a central processing unit (CPU) and an instruction decoder.

10. The method according to claim 1, further comprising the step of:

forwarding the plurality of decrypted instructions to a cache of the processor.

11. The method according to claim 1, wherein the method occurs within at least one of the following: a data switcher or router; a subscriber line interface card; a modem; a digitally-controlled machining tool; a portable radio; a wireless telephone; a voltmeter, ammeter, or ohmmeter; a personal digital assistant (PDA); a television; a cable or satellite TV set top box; a camcorder; a piece of audio/visual equipment; an audio compact disk (CD) system, player, or recorder; a digital versatile disk (DVD) system, player, or recorder; a piece of financial equipment, including at least one of a personal identification number (PIN) pad and a point of sale (POS) terminal; and a smart card.

12. A system for providing security to stored information, comprising:

at least one memory, said at least one memory storing a plurality of encrypted instructions, each encrypted instruction of the plurality of encrypted instructions associated with an address; and

a processor, said processor operatively coupled to said memory to retrieve the plurality of encrypted instructions therefrom; said processor including:

a first buffer, the first buffer capable of receiving the plurality of encrypted instructions;

a decryption unit, the decryption unit capable of receiving the plurality of encrypted instructions from the first buffer, the decryption unit adapted to decrypt the plurality of encrypted instructions using a decryption algorithm to produce a plurality of decrypted instructions;

a second buffer, the second buffer capable of receiving the plurality of decrypted instructions from the decryption unit; and

a processing area, the processing area capable of receiving at least one decrypted instruction of the plurality of decrypted instructions.

13. The system according to claim 12, wherein said processor comprises a microcontroller.

14. The system according to claim 12, wherein the processing area comprises at least one of a central processing unit (CPU) and an instruction decoder.

15. The system according to claim 12, wherein said processor further includes:

a cache memory, the cache memory capable of receiving the plurality of decrypted instructions from the second buffer.

16. The system according to claim 15, wherein the processing area is capable of receiving the at least one decrypted instruction of the plurality of decrypted instructions from the second buffer.

17. The system according to claim 16, wherein said processor further includes:

a memory controller, the memory controller capable of controlling movement of the plurality of decrypted instructions, the memory controller adapted to provide the processing area the at least one decrypted instruction from the second buffer and to provide the cache the plurality of decrypted instructions from the second buffer.

18. The system according to claim 17, wherein the memory controller is further adapted to provide the processing area the at least one decrypted instruction and the cache the plurality of decrypted instructions substantially simultaneously.

19. The system according to claim 17, wherein said processor further includes:

an address unit, the address unit capable of ascertaining a current instruction address, the address unit adapted to provide the instruction address to the memory controller; and

wherein the at least one decrypted instruction is associated with an instruction address "X" and another decrypted instruction of the plurality of decrypted instructions is associated with an instruction address "X+1"; and the memory controller is further adapted to provide the processing area the another decrypted instruction from the cache when the current instruction address corresponds to the instruction address "X+1".

20. The system according to claim 12, further comprising:

a bus, said bus operatively coupling said at least one memory to said processor; and

wherein a width of said bus is equivalent to a width of each encrypted instruction of the plurality of encrypted instructions.

21. The system according to claim 20, wherein the width of said bus and the width of each encrypted instruction is equal to eight (8) bits.

22. The system according to claim 15, wherein the cache is a two-way, set associative cache; and each block in each way of the cache is equal in length to a length of the second buffer.

23. The system according to claim 12, wherein the decryption unit is further adapted to decrypt the plurality of encrypted instructions substantially simultaneously.

24. The system according to claim 12, wherein the decryption algorithm comprises at least one of a data encryption standard (DES), a triple DES, and an advanced encryption standard (AES).

25. The system according to claim 12, wherein the first buffer comprises a latch that is capable of receiving the plurality of encrypted instructions sequentially directly from a bus coupling said at least one memory to said processor.

26. The system according to claim 12, wherein the system comprises at least one of the following: a data switcher or router; a subscriber line interface card; a modem; a digitally-controlled machining tool; a portable radio; a wireless telephone; a voltmeter, ammeter, or ohmmeter; a personal digital assistant (PDA); a television; a cable or satellite TV set top box; a camcorder; a piece of audio/visual equipment; an audio compact disk (CD) system, player, or recorder; a digital versatile disk (DVD) system, player, or recorder; a piece of financial equipment, including at least one of a personal identification number (PIN) pad and a point of sale (POS) terminal; and a smart card.

27. An arrangement for providing security to executable code stored in a memory external to a processor, the arrangement comprising:

memory means, said memory means storing a plurality of consecutive encrypted instructions;

means for sequentially receiving the plurality of consecutive encrypted instructions into a buffer means;

means for substantially simultaneously decrypting the plurality of consecutive encrypted instructions to create a plurality of consecutive decrypted instructions; and

means for distributing the plurality of consecutive decrypted instructions within the processor when requested by a processing entity.

28. The arrangement according to claim 27, wherein said means for distributing the plurality of consecutive decrypted instructions within the processor when requested by a processing entity includes means for transferring a decrypted instruction of the plurality of consecutive decrypted instructions to the processing entity when the processing entity presents an instruction address that is associated with the decrypted instruction.

29. The arrangement according to claim 28, further comprising:

cache means, said cache means for storing decrypted instructions; and

wherein said means for distributing the plurality of consecutive decrypted instructions within the processor when requested by a processing entity includes means, responsive to a processing entity request, for transferring the decrypted instruction from said cache means if the decrypted instruction is located therein upon receiving the processing request or for transferring the decrypted instruction prior to storing the decrypted instruction in said cache means if the decrypted instruction is not located therein upon receiving the processing entity request.

30. The arrangement according to claim 27, wherein the processor comprises a microcontroller.

31. The arrangement according to claim 30, wherein the microcontroller is compatible with the 8-bit "8051" instruction set.

32. The arrangement according to claim 27, wherein the arrangement comprises at least one of the following: a data switcher or router; a subscriber line interface card; a modem; a digitally-controlled machining tool; a portable radio; a wireless telephone; a voltmeter, ammeter, or ohmmeter; a personal digital assistant (PDA); a television; a cable or satellite TV set top box; a camcorder; a piece of audio/visual equipment; an audio compact disk (CD) system, player, or recorder; a digital versatile disk (DVD) system, player, or recorder; a piece of financial equipment, including at least one of a personal identification number (PIN) pad and a point of sale (POS) terminal; and a smart card.

33. The system according to claim 12, wherein the decryption unit is further adapted to decrypt the plurality of encrypted instructions using a decryption key formed responsive, at least partly, to at least a portion of the address associated with at least one encrypted instruction of the plurality of encrypted instructions.

34. The system according to claim 33, wherein:

the at least a portion of the address associated with at least one encrypted instruction of the plurality of encrypted instructions comprises an address value; and

the decryption unit is further adapted to form the decryption key by utilizing at least one of the following operations: (i) "xor"ing the address value with the decryption key, (ii) adding the address value to the decryption key, and (iii) applying at least one of the address value and the decryption key to a non-linear operation.

35. The arrangement according to claim 27, wherein said means for substantially simultaneously decrypting the plurality of consecutive encrypted instructions to create a plurality of consecutive decrypted instructions includes at least one decryption key; and

wherein said arrangement further comprises:

means for creating the at least one decryption key using at least a portion of an address associated with at least one encrypted instruction of the plurality of consecutive encrypted instructions.

36. The arrangement according to claim 27, wherein said memory means stores a plurality of corresponding encrypted checksums; and

wherein said arrangement further comprises:

means for comparing a calculated checksum to a corresponding decrypted checksum, the calculated checksum calculated from the plurality of consecutive decrypted instructions, and the corresponding decrypted checksum decrypted with the plurality of consecutive decrypted instructions from at least one corresponding encrypted checksum of the plurality of corresponding encrypted checksums.

37. The arrangement according to claim 36, wherein said arrangement further comprises:

means for thwarting an attacker's attempts to breach security, said means for thwarting an attacker's attempts to breach security becoming active when said means for comparing a calculated checksum to a corresponding decrypted checksum determines that the calculated checksum is not equivalent to the corresponding decrypted checksum.

38. An arrangement for providing information security with a processor, the arrangement comprising:

an encrypted buffer, said encrypted buffer capable of accepting a plurality of encrypted units and adapted to offer the plurality of encrypted units;

a decryptor, said decryptor capable of accepting the plurality of encrypted units and adapted (i) to decrypt the plurality of encrypted units to produce a plurality of decrypted units and (ii) to offer the plurality of decrypted units;

a decrypted buffer, said decrypted buffer capable of accepting the plurality of decrypted units and adapted to offer at least one of a single decrypted-buffer-originated decrypted unit of the plurality of decrypted units and the plurality of decrypted units;

a cache, said cache capable of accepting the plurality of decrypted units and adapted to offer a single cache-originated unit of the plurality of decrypted units;

a processing area, said processing area capable of accepting a decrypted unit of the plurality of decrypted units and adapted (i) to ascertain a program address and (ii) to offer the program address;

a controller, said controller capable of accepting the program address and adapted to control movement of the plurality of decrypted units; and

wherein said controller, at least partially, causes (i) said cache to offer the single cache-originated decrypted unit to said processing area if a first address associated with the single cache-originated decrypted unit corresponds to the program address and (ii) said decrypted buffer to offer the single decrypted-buffer-originated decrypted unit to said processing area and the plurality of decrypted units to said cache if a second address

associated with the single decrypted-buffer-originated decrypted unit corresponds to the program address.

39. The arrangement according to claim 38, wherein the arrangement comprises at least one of the following: a data switcher or router; a subscriber line interface card; a modem; a digitally-controlled machining tool; a portable radio; a wireless telephone; a voltmeter, ammeter, or ohmmeter; a personal digital assistant (PDA); a television; a cable or satellite TV set top box; a camcorder; a piece of audio/visual equipment; an audio compact disk (CD) system, player, or recorder; a digital versatile disk (DVD) system, player, or recorder; a piece of financial equipment, including at least one of a personal identification number (PIN) pad and a point of sale (POS) terminal; and a smart card.

40. The arrangement according to claim 38, wherein each unit comprises an instruction.

41. The arrangement according to claim 40, wherein each unit comprises a byte.

42. The arrangement according to claim 38, wherein a first length of a block of said cache is equivalent to a second length of the plurality of decrypted units.

43. The arrangement according to claim 38, wherein said decryptor is further adapted to decrypt the plurality of encrypted units to produce a plurality of decrypted units using at least one decryption key.

44. The arrangement according to claim 43, wherein the at least one decryption key is created, at least partially, responsive to at least a portion of the second address.

45. The arrangement according to claim 38, wherein the plurality of encrypted units and the plurality of decrypted units each comprise eight (8) bytes.

46. A method for providing enhanced security for a processor, comprising the steps of:

comparing a program address to at least one tag address of a cache to determine whether there is a hit;

if the hit is determined, then transferring at least one information unit from the cache to a processing area;

comparing the program address to an address corresponding to a decrypted buffer to determine whether there is a decrypted buffer match;

if the hit is not determined and the decrypted buffer match exists, then transferring another at least one information unit from the decrypted buffer to the processing area and transferring a plurality of information units from the decrypted buffer to the cache;

comparing the program address to an address corresponding to a decryption unit to determine whether there is a decryption unit match;

if the hit is not determined and the decrypted buffer match does not exist and the decryption unit match does exist, then decrypting another plurality of information units in the decryption unit and thereafter transferring the another plurality of information units from the decryption unit to the decrypted buffer and transferring yet another at least one information unit from the decrypted buffer to the processing area and transferring the another plurality of information units from the decrypted buffer to the cache.

47. The method according to claim 46, further comprising the steps of:

comparing the program address to an address corresponding to an encrypted buffer to determine whether there is an encrypted buffer match;

if the hit is not determined and the decrypted buffer match does not exist and the decryption unit match does not exist and the encrypted buffer match does exist, then transferring yet another plurality of information units from the encrypted buffer to the decryption unit and decrypting the yet another plurality of information units in the

decryption unit and thereafter transferring the yet another plurality of information units from the decryption unit to the decrypted buffer and transferring still yet another at least one information unit from the decrypted buffer to the processing area and transferring the yet another plurality of information units from the decrypted buffer to the cache.

48. The method according to claim 46, wherein the method occurs within at least one of the following: a data switcher or router; a subscriber line interface card; a modem; a digitally-controlled machining tool; a portable radio; a wireless telephone; a voltmeter, ammeter, or ohmmeter; a personal digital assistant (PDA); a television; a cable or satellite TV set top box; a camcorder; a piece of audio/visual equipment; an audio compact disk (CD) system, player, or recorder; a digital versatile disk (DVD) system, player, or recorder; a piece of financial equipment, including at least one of a personal identification number (PIN) pad and a point of sale (POS) terminal; and a smart card.

49. The arrangement according to claim 27, wherein said memory means stores a plurality of corresponding checksums; and

wherein said arrangement further comprises:

means for comparing a calculated checksum to a corresponding checksum of the plurality of checksums, the calculated checksum calculated from the plurality of

consecutive decrypted instructions, and the corresponding checksum is retrieved from said memory means in which it is stored clear and unencrypted.

50. A method for providing enhanced security for a processor, comprising the steps of:

ascertaining a program counter;

determining whether an instruction associated with an address that corresponds to the program counter is in a cache, a decrypted buffer, a decryption unit, or an encrypted buffer;

if so, forwarding the instruction;

if not,

retrieving a plurality of encrypted instructions from an external memory and loading the plurality of encrypted instructions into the encrypted buffer, the plurality of encrypted instructions including the instruction in an encrypted format;

forwarding the plurality of encrypted instructions from the encrypted buffer to the decryption unit;

decrypted the plurality of encrypted instructions in the decryption unit to produce a plurality of decrypted instructions, the plurality of decrypted instructions including the instruction in an unencrypted format;

forwarding the plurality of decrypted instructions from the decryption unit to the decrypted buffer; and

forwarding the instruction from the decrypted buffer for further processing.

51. The method according to claim 50, further comprising the step of:

forwarding the plurality of decrypted instructions from the decrypted buffer to the cache approximately during effectuation of said step of forwarding the instruction from the decrypted buffer for further processing.